Privacy class actions taking off

Volume of information collected, breaches cited as key factors

BY JULIUS MELNITZER
For Law Times

If there's any doubt that privacy class actions are on the verge of exploding, lawyers may want to consider the potential for significant new regulation in the area.

Last month, for example, the B.C. Freedom of Information and Privacy Association released a 123-page report on regulations for vehicle privacy. The report, noting the increasing availability of digital services in today's cars and trucks, recommended regulating privacy in automobiles. In response, lawyers Helen Fotinos, George Takach, and Kirsten Thompson, writing in an electronic bulletin from McCarthy Tétrault LLP, wondered whether other sectors of the economy are next.

It's easy to see why privacy advocates think the public needs more help from regulators. Statistics compiled by Christine Carron, Pamela Sidey, and Steve Tenai of Norton Rose Fulbright Canada LLP for a recent firm seminar suggest privacy breaches are already "prevalent and growing."

There's an irony here: the federal government is among the most notable offenders. The Norton Rose Fulbright lawyers report there were 5,600 privacy breaches by the federal government in 2014 that affected 44,000 individuals. Some 255 of the cases, affecting more than 36,000 individuals, were reported to the privacy commissioner.

Otherwise, data breaches from 2002 to 2012 affected the personal information of more than 725,000 Canadians; there were more than 400 health-related privacy violation complaints lodged with the Ontario information and privacy commissioner in each of 2012 and 2013; and 36 per cent of Canadian information technology professionals surveyed admitted their organization had had a significant breach in the last 12 months.

'We've just seen the beginning and we're likely to see a lot more,' says Steve Tenai.

Then there's the osmotic effect from the United States, where the Identity Theft Resource Center noted more than 5,000 reported data breaches since 2005 affecting 675 million records.

While hacking accounted for almost 30 per cent of the breaches in 2014, insider theft, data on the move, accidental exposure, subcontractor fault, employee negligence, and physical theft are all significant factors.

Business accounted for more than one-third of the breaches with the medical community falling victim some 27 per cent of the time followed by the government and military (16 per cent), the education sector (15 per cent), and the financial industry (eight per cent).

As Tenai sees it, the Ontario Court of Appeal's 2012 decision in *Jones v. Tsige*, which articulated the tort of intrusion on seclusion, paved the way for privacy class actions, some of which have already been certified and some of which have settled. "We've just seen the beginning and we're likely to see a lot more," says Tenai.

"*Jones* was a case about intentional conduct, premised on intention and recklessness, and what has followed are class actions that involve a deliberate breach of privacy rights, including employees acting improperly or in breach of what might be expected of them."

Evans v. The Bank of Nova Scotia, for example, involved an employee alleged to have accessed information about mortgage applicants and passed them on to his girlfriend who subsequently sold the information to a third party for improper purposes. The Divisional Court recently dismissed the bank's application for leave to appeal the certification order.

"*Evans* potentially extends the tort of intrusion upon seclusion to include vicarious liability claims," says Tenai.

Then there are the cases involving cyber security breaches or hackers. Companies sued include Sony, Winners, and HomeSense. A series of class actions have emerged alleging that the security of Apple's operating system was inadequate for the protection of personal information.

Lost data can also result in significant class actions. In Quebec, the Superior Court recently authorized a national class action for damages against TD Auto Finance (formerly DaimlerChrysler) for losing personal data on a non-encrypted tape misplaced by the commercial courier company transporting it from the United States.

As well, alleged breaches can include the way companies use information they have validly obtained. "That may be the most significant direction in which we're moving," says Tenai, citing a recent case filed against Facebook in British Columbia. "Facebook used the names and photos of certain individuals in sponsored sites without obtaining consent and that's now under attack."

While *Jones* has been instrumental in the emergence of privacy class actions, plaintiff's counsel haven't been lacking in creativity in expanding the decision's ambit.

"We're seeing cases where the privacy complaint is being framed in breach of contract, breach of warranty, and negligence," says Tenai.

"The boundaries have not yet been fully set because we're only at the certification stage in these cases, so only a limited review of the merits is involved."

Also driving privacy class actions is the fact that class members don't have to prove pecuniary damages in the sense of out-of-pocket losses.

"Emotional upset or inconvenience can suffice," says Tenai.

"And although the *Jones* court set a cap of about $20,000, a large class can produce awards that are very significant."

By way of example, more than 14,000 new mothers whose personal data was allegedly sold to private educational savings companies by two employees at the Rouge Valley Health System are suing for some $412 million.

"Electronics record systems are increasingly central to our daily lives, whether in the form of school grades, bank records or hospital charts," says Anne Posno of Lenczner Slaght Royce Smith Griffin LLP.

"As a corollary, we are now more exposed than ever to breaches of privacy involving intimate personal details."

Recently, the appeal court removed a considerable potential barrier to class actions based on information covered by Ontario's Personal Health Information Protection Act. "The legislation includes detailed provisions on handling complaints and speaks to the availability of certain remedies through the office of the information and privacy commissioner," says Posno.

"In *Hopkins v. Kay*, the Court of Appeal was forced to determine whether [the act] ousted the availability of a civil action when the privacy breach concerned health records."

In deciding the legislation didn't oust the common law remedy, the Court of Appeal opened the door to the sustainability of privacy claims that intrude on regulated arenas.

"It's not that unusual because we face duplicative proceedings involving regulatory bodies all the time," says Posno.

"Having said that, I don't think *Hopkins* opens the floodgates so much as it solidifies the determination of how to pursue remedies for such breaches."

Still, *Hopkins* is contrary to decisions in Alberta and British Columbia. "Ultimately, the Supreme Court may have to decide the issue," says Posno.

In the meantime, the steady growth of privacy class actions may be an unstoppable trend.

"It was bound to happen both because of the sheer volume of personal information that is being collected and because of the number of breaches that have occurred," says Posno.

Then, of course, there's Canada's new anti-spam legislation: the provisions allowing a private right of action come into force in 2017. **LT**